THE DIOPHANTINE EQUATION $x^2+3=y^n$

by J. H. E. COHN

(Received 2 December, 1991)

Introduction. Many special cases of the equation $x^2+C=y^n$ where x and y are positive integers and $n \geqslant 3$ have been considered over the years, but most results for general n are of fairly recent origin. The earliest reference seems to be an assertion by Fermat that he had shown that when $C=2$, $n=3$, the only solutions are given by $x=5$, $y=3$; a proof was published by Euler [**1**]. The first result for general n is due to Lebesgue [**2**] who proved that when $C=1$ there are no solutions. Nagell [**4**] generalised Fermat's result and proved that for $C=2$ the equation has no solution other than $x=5$, $y=3$, $n=3$. He also showed [**5**] that for $C=4$ the equation has no solution except $x=2$, $y=2$, $n=3$ and $x=11$, $y=5$, $n=3$, and claims in [**6**] to have dealt with the case $C=5$. The case $C=-1$ was solved by Chao Ko, and an account appears in [**3**], pp. 302–304.

The method for $C=1$, 2 or 4 consists of two parts. Firstly, using the fact that the fields $\mathbb{Q}[\sqrt{-1}]$ and $\mathbb{Q}[\sqrt{-2}]$ have unique prime factorisation it is shown that $y=a^2+C$ for some suitable a. Then the fact that the fundamental unit in the field $\mathbb{Q}[\sqrt{(a^2+C)}]$ can be expressed simply in terms of a is used. For other values of C, even if the first step can be followed, the second cannot, and a different method is required to complete the proof. Nagell [**6**] found such a method for $C=8$, and proved that there are no solutions.

It follows from [**8**, Theorem 12.2], an extension of a deep analytical result due to Shorey, van der Poorten, Tijdeman and Schinzel [**7**], that *any* such equation has but finitely many solutions, and moreover that these are effectively computable, in the usual sense, viz., that it is possible to find them all by considering all values of say, x, up to some bound $K(C)$ which can be explicitly calculated. In practice, the power of that method is limited by the huge size of the K that arises, but it does provide a theoretical method for solving such problems.

THEOREM. *The equation $x^2+3=y^n$ has no solution in positive integers x, y and $n \geqslant 3$.*

Proof. The case in which n is even is easily dismissed, since then 3 is to be expressed as the difference of two integer squares; this implies $x=1$ which gives no solution. For n odd there is no loss of generality in considering only odd primes p. If x were odd then $x^2+3 \equiv 4 \pmod 8$, yielding no solution. Thus x is even, and then $y \equiv 3 \pmod 4$, and so in the field $\mathbb{Q}(\sqrt{-3}]$ with unique prime factorisation

$$(x+\sqrt{-3})(x-\sqrt{-3})=y^p,$$

where the factors on the left hand side have no common factor. Thus for some rational integers A and B with the same parity

$$x+\sqrt{-3}=\varepsilon(\tfrac{1}{2}(A+B\sqrt{-3}))^p$$

and $y=\frac{1}{4}(A^2+3B^2)$, where ε is a unit of the field. Since there are just six units, ± 1, $\pm\omega$, $\pm\omega^2$, where $\omega=\exp(2\pi i/3)$, all of which satisfy $\varepsilon^6=1$, it follows that if $p \neq 3$ these can be absorbed into the pth power, and so we find that

$$x+\sqrt{-3}=(\tfrac{1}{2}(A+B\sqrt{-3}))^p. \qquad (1)$$

https://doi.org/10.1017/S0017089500009757 Published online by Cambridge University Press

On the other hand, for $p=3$, we cannot necessarily do this, and obtain in addition two more cases, viz.,

$$x+\sqrt{-3}=\tfrac{1}{2}(1\pm\sqrt{-3})(\tfrac{1}{2}(A+B\sqrt{-3}))^3. \tag{2}$$

We deal with (2) first. Equating imaginary parts yields

$$16=\pm(A^3-9AB^2)+(3A^2B-3B^3)$$

and we can ignore the lower sign by absorbing it into A if necessary. Then $16=A^3+3A^2B-9AB^2-3B^3=(A+B)^3-12AB^2-4B^3$. Since A and B have the same parity, we write $2C=A+B$, and obtain $2=C^3-3B^2C+B^3$. This is easily seen to be impossible, since the right hand side is odd unless both B and C are even, and is divisible by 8 if they are. So this case does not arise.

Equating imaginary parts in (1), we obtain

$$2^p=B\sum_{r=0}^{\frac{1}{2}(p-1)}\binom{p}{2r+1}A^{p-2r-1}(-3B^2)^r.$$

If B were odd, then $B=\pm1$, and then modulo p, we should find that $2\equiv2^p\equiv\pm(-3)^{\frac{1}{2}(p-1)}\equiv\pm(-3\mid p)$, which is impossible. So A and B are both even, and so substituting $A=2a$, $B=2b$ gives

$$1=b\sum_{r=0}^{\frac{1}{2}(p-1)}\binom{p}{2r+1}a^{p-2r-1}(-3b^2)^r,$$

and so $b=\pm1$, $y=a^2+3$. Since $y\equiv3\pmod 4$, a is even and

$$\pm1=\sum_{r=0}^{\frac{1}{2}(p-1)}\binom{p}{2r+1}a^{p-2r-1}(-3)^r,$$

and we may reject the lower sign modulo 4. Hence

$$1=\sum_{r=0}^{\frac{1}{2}(p-1)}\binom{p}{2r+1}a^{p-2r-1}(-3)^r. \tag{3}$$

Thus $3\nmid a$ and $p\equiv1\pmod 3$. Now let $\xi=a^2-1$. Then the right hand side of (3) becomes

$$f_p(\xi)=\sum_{r=0}^{\frac{1}{2}(p-1)}\binom{p}{2r+1}(\xi+1)^{\frac{1}{2}(p-2r-1)}(-3)^r=\sum_{r=0}^{\frac{1}{2}(p-1)}A_r\xi^r,$$

say, where $A_0, A_1, \ldots, A_{\frac{1}{2}(p-1)}$ are integers. Since $p\equiv1\pmod 6$, let $3^\nu\,\|\,(p-1)$. We assert that:

$$A_0=2^{p-1};\qquad A_1=0;\qquad A_2=-p(p-1)\,.\,2^{p-6};\qquad 3^{\nu+2-r}\mid A_r,\qquad 3\leqslant r\leqslant\nu+2,$$

which we prove below. Subject to these assertions, we can now complete the proof. For we then have from (3)

$$2^{p-1}-1=p(p-1)\,.\,2^{p-6}(a^2-1)^2-\sum_{r=3}^{\frac{1}{2}(p-1)}A_r(a^2-1)^r$$

and this is impossible as the left hand side is divisible by precisely $3^{\nu+1}$ whereas every term on the right is divisible by at least $3^{\nu+2}$.

To prove the assertion we shall expand $f_p(\xi)$ as a Taylor series. This will be valid for

https://doi.org/10.1017/S0017089500009757 Published online by Cambridge University Press

all ξ, since it terminates. Define for all positive integers m the real function

$$f_m(\xi)=\frac{((1+\xi)^{\frac{1}{2}}+\sqrt{-3})^m-((1+\xi)^{\frac{1}{2}}-\sqrt{-3})^m}{2\sqrt{-3}}. \tag{4}$$

Then for $m\geqslant 3$,

$$f_m(\xi)=2(1+\xi)^{\frac{1}{2}}f_{m-1}(\xi)-(4+\xi)f_{m-2}(\xi) \tag{5}$$

and

$$\begin{aligned} f_m(0)&=\frac{(1+\sqrt{-3})^m-(1-\sqrt{-3})^m}{2\sqrt{-3}}\\ &=\frac{(-2\omega^2)^m-(-2\omega)^m}{2(\omega-\omega^2)}\\ &=-(-2)^{m-1}\frac{\omega^{2m}-\omega^m}{\omega-\omega^2}\\ &=\begin{cases} 0 & \text{if } m\equiv 0 \pmod 3)\\ (-2)^{m-1} & \text{if } m\equiv 1 \pmod 3).\\ -(-2)^{m-1} & \text{if } m\equiv 2 \pmod 3)\end{cases} \end{aligned} \tag{6}$$

Thus since $p\equiv 1 \pmod 6$ we obtain immediately $A_0=f_p(0)=2^{p-1}$. Differentiating (4) yields

$$2(1+\xi)^{\frac{1}{2}}f'_m(\xi)=mf_{m-1}(\xi), \tag{7}$$

and so from (6), $A_1=f'_p(0)=0$ since $p-1\equiv 0 \pmod 6$. Again

$$4(1+\xi)^{\frac{1}{2}}\frac{d}{d\xi}\{(1+\xi)^{\frac{1}{2}}f'_m(\xi)\}=m(m-1)f_{m-2}(\xi)$$

yielding

$$4(1+\xi)f''_m(\xi)+2f'_m(\xi)=m(m-1)f_{m-2}(\xi) \tag{8}$$

and so $4f''_p(0)=-p(p-1)2^{p-3}$ in view of (6), since $p-2\equiv 5 \pmod 6$. Thus $A_2=-p(p-1)2^{p-6}$. Now use (7) and (8) in (5) to obtain

$$4(\xi^2+5\xi+4)f''_p(\xi)-2\{\xi(2p-3)+(2p-6)\}f'_p(\xi)+p(p-1)f_p(\xi)=0.$$

Now let $r!A_r=f_p^{(r)}(0)=2^{p-2r-1}p(p-1)B_r$. Then the above equation yields without difficulty $B_1=0$, $B_2=-1$ and for $r>0$ $B_{r+2}=(p-5r-3)B_{r+1}-(p-2r)(p-2r-1)B_r$. Thus B_r is an integer for each $r\geqslant 1$. Hence $r!A_r=f_p^{(r)}(0)$ is divisible by $(p-1)$ and in particular by 3^ν. But the power of 3 dividing $r!$ is $\sum_{\rho=1}^{\infty}[r/3^\rho]\leqslant r-2$, which completes the proof.

REFERENCES

1. L. Euler, *Algebra*, *Volume 2.*

2. V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m=y^2+1$, *Nouvelles Annales des Mathématiques* (1) **9** (1850) 178.

https://doi.org/10.1017/S0017089500009757 Published online by Cambridge University Press

3. L. J. Mordell, *Diophantine equations* (Academic Press, 1969).

4. T. Nagell, Verallgeminerung eines Fermatschen Satzes, *Archiv der Mathematik* **5** (1954), 153–159.

5. T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Regiae Soc. Sc. Upsaliensis* (4) **16** No. 2 (1955), 1–38.

6. T. Nagell, On the Diophantine equation $x^2+8D=y^n$, *Arkiv för Matematik* **3** (1955), 103–112.

7. T. N. Shorey, A. J. van der Poorten, R. Tijdeman and Schinzel, Applications of the Gel'fond–Baker method to diophantine equations, in *Transcendence Theory: Advances and Applications*, (Academic Press, 1977), 59–77.

8. T. N. Shorey and Tijdeman, *Exponential Diophantine equations*, (Cambridge University Press, 1986).

Department of Mathematics,
RHBNC
Egham
Surrey TW20 0EX.

https://doi.org/10.1017/S0017089500009757 Published online by Cambridge University Press